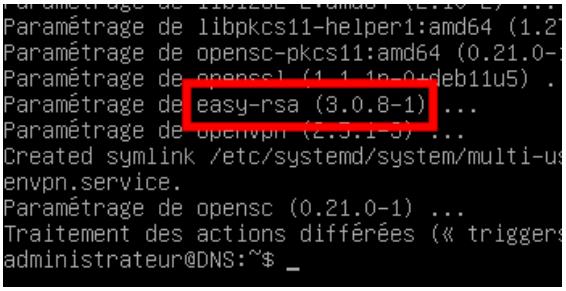
VPN

1) Installation OpenVPN et Easy-RSA

```
sudo apt install openvpn
mkdir /etc/openvpn/easy-rsa
cd /etc/openvpn/easy-rsa/
sudo apt install wget
```



Télécharger le ficher EasyRSA correspondant à la version installée par le système

```
sudo wget https://github.com/openvpn/easy-rsa/releases/download/v3.0.8/easyrsa-3.0.8.tgz
sudo tar -xvzf easyrsa-3.0.8.tgz
cd EasyRSA-3.0.8
sudo mv * ../
cd ..
sudo rm -rf EasyRSA-3.0.8
sudo rm easyrsa-3.0.8.tz
```

2) Création du Certificat d'autorité

```
sudo cp vars.example vars
sudo nano vars
```

On va décommenter et modifier les lignes suivantes et créer celles qui ne sont pas inscrites

```
set_var EASYRSA                 "$PWD"
set_var EASYRSA_PKI             "$EASYRSA/pki"
set_var EASYRSA_DN              "cn_only"
set_var EASYRSA_REQ_COUNTRY     "FR"
set_var EASYRSA_REQ_PROVINCE    "Isere"
set_var EASYRSA_REQ_CITY        "Grenoble"
set_var EASYRSA_REQ_ORG         "Entreprise d'autorité de certification"
set_var EASYRSA_REQ_EMAIL       "admin@exemple.com"
set_var EASYRSA_REQ_OU          "Entreprise cliente du certificat"
set_var EASYRSA_KEY_SIZE        2048
set_var EASYRSA_ALGO            rsa
set_var EASYRSA_CA_EXPIRE 3650  # nombre de jours avant expiration du certificat d'autorité
set_var EASYRSA_CERT_EXPIRE     365 # nombre de jours avant expiration du certificat client
set_var EASYRSA_NS_SUPPORT      "no"
set_var EASYRSA_NS_COMMENT      "Entreprise d'autorité de certification" # commentaire à afficher
set_var EASYRSA_EXT_DIR         "$EASYRSA/x509-types"
set_var EASYRSA_DIGEST          "sha256"
```

```
sudo ./easyrsa init-pki
sudo ./easyrsa build-ca nopass # donner un nom au certificat d'autorité
```

3) Génération du certificat serveur et les fichiers clés

```
sudo ./easyrsa gen-req vpnserver nopass # donner un nom au certificat du serveur
sudo ./easyrsa gen-dh # génération clé diffie-hellman
sudo ./easyrsa sign-req server vpnserver
```

Nota : remplacer vpnserver par le nom que vous avez donné au certificat d'autorité

On copie les fichiers générés dans le dossier destiné à la configuration serveur

Nota : pour cette partie, on doit s'authentifier en tant que super utilisateur avec le commande su

```
cp pki/ca.crt /etc/openvpn/server/
cp pki/dh.pem /etc/openvpn/server/
cp pki/private/vpnserver.key /etc/openvpn/server/
cp pki/issued/vpnserver.crt /etc/openvpn/server/
exit
```

4) Génération du certificat client et les fichiers clés

```
sudo ./easyrsa gen-req vpnclient nopass # donner un nom au certificat client
sudo ./easyrsa sign-req client vpnclient
```

On copie les fichiers générés dans le dossier destiné à la configuration serveur

Nota : pour cette partie, on doit s'authentifier en tant que super utilisateur avec le commande su

```
cp pki/ca.crt /etc/openvpn/client/
cp pki/private/vpnclient.key /etc/openvpn/client/
cp pki/issued/vpnclient.crt /etc/openvpn/client/
exit
```

5) Configuration du serveur openvpn

Créer le fichier de configuration

```
sudo nano /etc/openvpn/server.conf
```

et saisir les informations suivantes

```
port 1194 # port par défaut du VPN
proto udp
dev tun
ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/vpnserver.crt
key /etc/openvpn/server/vpnserver.key
dh /etc/openvpn/server/dh.pem
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 1.1.1.1"

cipher AES-256-CBC
tls-version-min 1.2
tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-SHA256:TLS-DHE-RSA-
WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
auth SHA512
auth-nocache
keepalive 20 60
persist-key
persist-tun
daemon
user nobody
group nogroup
log-append /var/log/openvpn.log
verb 3
```

Nota : il est préférable d'utiliser le protocole UDP pour le VPN, sinon utiliser la ligne proto tcp-server pour la configuration serveur et proto tcp-client pour la configuration du client

Nota : l'option « local » permet de préciser sur quelle carte réseau fournir le service VPN (exemple : local 192.168.0.1)

On active le service au démarrage

```
systemctl start openvpn@server
systemctl enable openvpn@server
```

on vérifie que l'interface réseau VPN est bien créée

```
ip -c a
```

on doit trouver une carte réseau virtuelle tun0

6) Activer IP forwarding

```
sudo nano /etc/sysctl.conf
```

décommenter la ligne

```
net.ipv4.ip_forward = 1
```

redémarrer le service

```
sysctl -p
```

7) Installation et configuration OpenVPN sur un client Linux

Installation du client openvpn

```
sudo apt install openvpn
```

Installation de openssh sur le client

```
sudo apt install openssh-client
```

Installation de openssh sur le serveur

```
sudo apt install openssh-server
```

On rajoute les droits de lecture pour pouvoir les copier à partir du serveur

```
sudo chmod 604 /etc/openvpn/client/*
```

On lance la copie à partir du client

```
sudo scp user@adresseIP:/etc/openvpn/client/* /etc/openvpn/client/
```

Nota : user est le nom du compte utilisé sur le serveur

Nota : adresseIP est l'adresse IP du serveur

on créée le fichier ovpn sur le client

```
sudo nano /etc/openvpn/client/client.ovpn
```

on copie les données suivantes

```
client
dev tun
proto udp
remote adresseIPduserveur 1194
ca /etc/openvpn/client/ca.crt
cert /etc/openvpn/client/vpnclient.crt
key /etc/openvpn/client/vpnclient.key
cipher AES-256-CBC
data-ciphers-fallback AES-256-CBC
auth SHA512
auth-nocache
tls-version-min 1.2
tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-SHA256:TLS-DHE-RSA-
WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
resolv-retry infinite
nobind # permet la connection à plusieurs VPN en simultané
persist-key
persist-tun
mute-replay-warnings
verb 3
```

Nota : il est possible de mettre plusieurs serveurs VPN en rajoutant des lignes «remote adresseIPduserveur 1194 ». Le service va se connecter au suivant si le premier ne répond pas.

8) Installation et configuration OpenVPN sur un client Windows

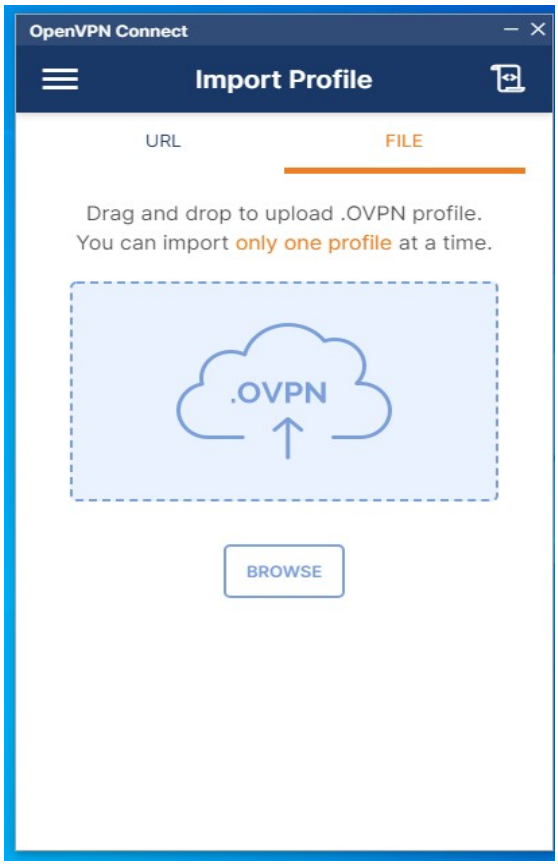
Télécharger OpenVPN depuis le site officiel de l'éditeur et l'installer.

Télécharger les certificats depuis le serveur à l'aide d'une fenêtre CMD

```
scp user@adresseIP:/etc/openvpn/client/* c:/Chemin/Du/Dossier/
```

Créer le fichier de configuration client.ovpn

```
client
dev tun
proto udp
remote adresseIPduserveur 1194
ca c:\\Chemin\\Du\\Dossier\\ca.crt
cert c:\\Chemin\\Du\\Dossier\\vpnclient.crt
key c:\\Chemin\\Du\\Dossier\\vpnclient.key
cipher AES-256-CBC
data-ciphers-fallback AES-256-CBC
auth SHA512
auth-nocache
tls-version-min 1.2
tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-SHA256:TLS-DHE-RSA-
WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
resolv-retry infinite
nobind
persist-key
persist-tun
mute-replay-warnings
verb 3
```



Importer le fichier client.ovpn